UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,424	06/24/2003	Branislav N. Meandzija	15685P208	3310

45222 7590 08/22/2007
ARRAYCOMM/BLAKELY
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
08/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,424	MEANDZIJA ET AL.	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2007 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24,26-40 and 42-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-22,26-38,42-49* is/are rejected.

7)☒ Claim(s) *7,8,23,24,39 and 40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on June 08, 2007 has been entered. Claims 1-24, 26-40, 42-49 are pending. Claims 25 and 41 are canceled by the applicant and claims 1, 10, 17, 26, 33 and 42 are also amended by the applicant.

2. The Office would like to notify the Applicant that, there has been a change in the Examiner to conduct the future examination and prosecution process of the currently pending application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 4-6, 9, 10-13, 17, 20-22, 26-29, 33, 36-38, 42-45 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer (Us patent 6,009,173) and in view of Kaliski Jr. (US patent 6,189,098).

As per claims 1, 17 and 33, Summer teaches a method, a user terminal and a machine-readable medium performed by a user terminal of a wireless access network, the method comprising: generating a shared secret to be provided to an access point of the wireless access network (Fig. 3, step 108, where sender-receiver session key is

disclosed, see also col. 3, lines 32-34); encrypting the shared secret with an access point public key (col. 3, lines 34-45, where the session key is encrypted using receiver's public key); sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the authenticator string (col. 3, lines 33-52);

Summer teaches generating a digest of the message and encrypting the digest using his signature key [col. 3 lines 26-28 i.e. generating an authenticator string encrypted with a user terminal private key]. Summer doesn't expressively mention authenticator string including a portion of the shared secret.

However, Kaliski teaches the authenticator string including a portion of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver and (CERT-C)KSS).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kaliski with Summer, since one would have been motivated to provide safeguard s against a third party impersonating the user terminal by simply replaying copies of the previous signatures intercepted or acquired (Kaliski, Jr., col. 1, lines 30-42).

As per claims 4, 20 and 36, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claims 1, 17 and 33, wherein generating the authenticator string comprises generating an authenticator message and signing the authenticator message with the user terminal private key (Summer, col. 3, lines 26-28).

As per claims 5, 21 and 37, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively, wherein signing the authenticator message comprises: generating a digest of the authenticator message (Summer, col. 3, lines 24-26); and encrypting the authenticator message digest with the user terminal private key (Summer, col. 3, lines 26-28).

As per claims 6, 22 and 38, Summer teaches the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively. Summer does not teach but Kaliski, Jr. discloses wherein the authenticator message comprises a time parameter and at least part of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver and (CERT-C)KSS).

As per claims 9, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claim 1, wherein the user terminal generates and encrypts the shared secret prior to identifying the access point by encrypting the shared secret with the public keys of a plurality of access points stored in the user terminal [Summer, col. 3 lines 34-35].

As per claims 10 and 42, Kaliski, Jr. teaches a method, a machine-readable medium performed by an access point of a wireless access network, comprising: receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, a user terminal certificate, (col. 3, lines 53-65); decrypting the shared secret using an access point private key (col. 3, lines 54-55); authenticating the user terminal by checking the

authenticator string using a user terminal public key included in the user terminal certificate to verify possession of the user terminal private key by the user terminal (col. 4, lines 1-24).

Summer teaches generating a digest of the message and encrypting the digest using his signature key [col. 3 lines 26-28 i.e. generating an authenticator string encrypted with a user terminal private key]. Summer doesn't expressively mention authenticator string including a portion of the shared secret.

However, Kaliski teaches the authenticator string including a portion of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver and (CERT-C)KSS).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kaliski with Summer, since one would have been motivated to provide safeguard s against a third party impersonating the user terminal by simply replaying copies of the previous signatures intercepted or acquired (Kaliski, Jr., col. 1, lines 30-42).

As per claims 11 and 43, Summer and Kaliski teach the method and the machine-readable medium of claims 10 and 42 respectively, wherein the user terminal certificate is scrambled, and the access point unscrambles the user terminal certificate using the shared secret (col. 3, lines 56-59).

As per claims 12 and 44, Summer and Kaliski teach the method and the machine-readable medium of claims 10 and 42 respectively, wherein checking the

authenticator string comprises decrypting the authenticator string using the user public key (Summer, col. 4, lines 15-24).

As per claims 13 and 45, Summer and Kaliski teach the method and machine-readable medium of claims 12 and 45 respectively, wherein checking the authenticator string further comprises generating and authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string (Summer, col. 4, lines 19-24).

As per claims 49, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claim 1, generating a digest of the message and encrypting the digest using his signature key [col. 3 lines 26-28 i.e. generating an authenticator string encrypted with a user terminal private key]. Summer doesn't expressively mention authenticator string including a portion of the shared secret. However, Kaliski teaches the authenticator string including a portion of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver and (CERT-C)KSS).

As per Claims 26-29,correspond to an access point performing the steps recited method claims 10-12. Claims 26-29 are rejected for the same reason provided in the statement of rejections of claims 10-13 above.

4. Claims 2, 3, 14-16, 18, 19, 30-32, 34, 35 and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer (Us patent 6,009,173) in view of Kaliski Jr. (US patent 6,189,098) and in view of Persson et al. (US patent 6,754,824).

As per claims 2, 18 and 34, Summer and Kaliski teaches the method, the user terminal and the machine-readable medium of claims 1, 17 and 33 respectively, except wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

However, in an analogous art, Persson is directed to telecommunications systems and methods wherein the identity of the transmitting node is verified by modulating the CRC code utilizing a sequence known only to the participating parties. The modified CRC is generated by both the transmitting node and the receiving node initializing a LFSR register by a common key known only to the participating nodes (i.e. a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secrete (Persson, col. 2, lines 5-23).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to employ the teachings of Persson within the method and system of Summer and Kaliski for combining Kaliski's certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret in order to verify both the authenticity of the received certificate and the identity of transmitting node and to deter unauthorized party to replace the participating nodes if week encryption or no encryption is switched on after authentication (Persson, col. 1, lines 35-49).

As per claims 3, 19 and 35, once modified, Summer teaches the method, the user terminal and the machine-readable medium of claims 2, 18 and 34 respectively, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point (Kaliski, Jr., col. 4, lines 42-55, i.e. KSS is used for symmetric key cryptography, the remainder of KSS||TS).

As per claims 14 and 46, Summer teaches the method and the machine-readable medium of claims 13 and 45 respectively. Summer does not teach but Kaliski, Jr. discloses wherein the authenticator message comprises at least part of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver). It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Kaliski, Jr. into the method and system of Summer to include at least part of the shared secret in the authenticator message to provide safeguard s against a third party impersonating the user terminal by simply replaying copies of the previous signatures intercepted or acquired (Kaliski, Jr., col. 1, lines 30-42).

As per claims 15 and 47, Kaliski Jr. teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein the user terminal certificate is signed by a certificate authority trusted by the access point (col. 3, lines 63-67).

As per claims 16 and 48, Once modifies, Summer teaches the method and the machine-readable medium of claims 10 and 42, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user terminal (Kaliski

Jr. col. 4, lines 39-55, the shared secret session key KSS is used for symmetric key encryption between the client and the server).

As per Claims 30-32, correspond to an access point performing the steps recited in method claims 14-16. Claims 30-32 are rejected for the same reason provided in the statement of rejections of claims 14-16 above above.

Response to Amendment

5. Applicant has amended claims 1, 10, 17, 26, 33 and 42. Claims 1, 10, 17, 26, 33 and 42 have been modified to include the limitation "including a portion of the shared secret encrypted with a user terminal private key". The present application has been reassigned to the present examiner, who has thoroughly reviewed and searched the present invention. The cited prior art Summer and Kaliski teaches the amended claim limitation as above. See rejection above.

Allowable Subject Matter

6. Claims 7, 8, 23, 24, 39 and 40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

7. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP

8/17/07

KIM VU
SUPERVISORY PATENT EXAM
TECHNOLOGY CENTER 2100